REMARKS

I. Introduction

In response to the Office Action dated July 10, 2008, claims 22 and 26 have been cancelled, claims 1, 19 and 25 have been amended, and new claims 28-32 have been added. Claims 1-5, 11-19, 21, 23-25 and 27-32 are in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Prior Art from Related Cases

According to MPEP §§2001.06(b), 609.02, the Examiner will consider prior art cited in earlier continuation applications, and must indicate in the first Office Action whether the prior art cited in the related earlier application has been reviewed.

The Applicant note that this application is a continuation of one or more parent or sibling applications. Accordingly, the Applicant respectfully request that the Examiner indicate that a review of the related cases has been undertaken and the prior art cited and arguments made in those applications has been considered.

III. Office Action Objections

In paragraph (3), claim 26 is objected to under 37 C.F.R. §1.75(c) as being of improper dependent form for failing to further limit the subject matter of a previous claim. The Applicants have canceled claim 26.

IV. The Cited References and the Subject Invention

A. The Schier Reference

U.S. Patent No. 6,907,123, issued June 14, 2005 to Schier discloses a secure voice communication system. A secure real time voice communication system 70 is provided that allows for the secure transmission of voice communications between a sending device 72 and a receiving device 78 through the public switch telephone network 76. The device 72 uses an encryption decryption engine 30 which is capable of executing a number of encryption algorithms which are selected using an encryption selection table 80. An encryption key can be calculated from a periodic key value and a public variable key value. Further, the encryption algorithm used can be periodically changed during a voice communication session so that multiple encryption techniques can be used within the same communication session.

B. The Wasilewski Reference

U.S. Publication No. 2002/0094084, issued July 18, 2002 to Wasilewski et al. discloses a method and apparatus for providing conditional access in connection-oriented interactive networks with a multiplicity of service providers. Methods and apparatus are described for ensuring that programs comprising at least one of video, audio, and data that are requested by a customer from a service provider (SP) via an interactive information services system, which transmits the requested programs in program bearing packets to a set top unit (STU) associated with the customer, are accessible by only authorized customers. The apparatus is positioned between the SP and the STU and comprises: means for receiving the program beating packets in a first network protocol from a first data link and removing the packets from the first network protocol; means for adding conditional access to the program bearing packets; and, means for re-encapsulating the program bearing packets in a second network protocol and outputting the program bearing packets over a second data link. Methods and apparatus for applying conditional access are described that comprise encrypting selected program bearing packets with a first key; encrypting the first key with a second key; and, encrypting the second key according to a public-key encryption algorithm using a public key corresponding to a private key stored within the STU associated with the customer.

C. The Gungle Reference

U.S. Patent No. 5,912,453, issued June 15, 1999 to Gungle discloses a multiple application chip card with decoupled programs. The integration of multiple application programs on one chip card is described, whereby the application programs stored on it do not have access to each other, which is achieved through a separation and de-coupling of the individual programs from one another. A first embodiment has several mutually-independent units, consisting respectively of a processor unit and a memory unit. Communication of these independent units with the external world and also with each other takes place through a control unit. A communication of the independent units with each other can only take place through the respective processor units, so that the linked memory units may not be accessed by circumvention of the processor unit. In a further embodiment, the separation of different applications on a chip card with only one processor takes place through the insertion of a separation of the application segments in the memory area of the chip card. The separation has as a result that each application may only access one predetermined area within the memory, and that access outside of the specified memory area is disabled for this application.

D. The Davis Reference

U.S. Patent No. 6,064,739, issued May 16, 2000 to Davis discloses a system and method for copy-protecting distributed video content. A secure video content processor ("SVCP") which receives encrypted digital video information and converts it into analog information for a monitor while preventing unauthorized access to the intermediate unencrypted digital data. The SVCP uses hardware envelopes to prevent unauthorized access to the decrypted digital stream. When a need arises to transmit digital data outside the hardware envelope, the digital data is encrypted and then decrypted when it re-enters a hardware protected section of circuitry.

E. The Joly Reference

U.S. Patent No. 7,162,034, issued January 9, 2007 to Joly discloses a method and apparatus for multi-session time-slot multiplexing. Techniques for performing multistage processing with feedback include a multi-stage feedback processor comprising a first plurality of processing stages connected in series. A feedback channel connects a last stage to one of the other stages. Each processing stage is configured to process one block of data from a data stream during one processing cycle. A parallel input queue includes a second plurality of input queues connected in parallel to the first stage. The parallel input queue directs a block to the first stage alternately from each of a third plurality of data streams. In an embodiment, the number of data streams is no greater than the number of input queues. This arrangement significantly improves throughput for multistage processing with feedback. The arrangement is suitable for encryption and decryption of network traffic using block-based symmetric ciphers.

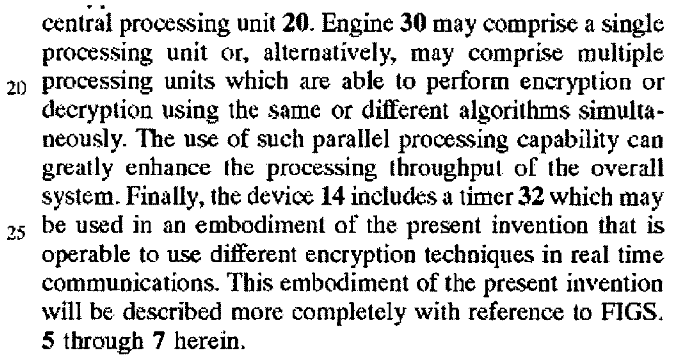
V. Office Action Prior Art Rejections

In paragraph (9), the Office Action rejected claims 1, 2, 4, 5, 11, 12, 15, 16, 19 and 22-27 under 35 U.S.C. §103(a) as unpatentable over Schier, U.S. Patent 6,907,123 (Schier) in view of Wasilewski et al., U.S. Publication 2002/0094084 (Wasilewski).

With Respect to Claims 1, 19 and 25: Claim 1 recites:

> *A conditional access module, configured to control access to a media program via a receiver communicably coupleable to the conditional access module, comprising:*
>
> *a first processor;*
>
> *a second processor; and*
>
> *an interface module, communicatively coupled to the first processor and the second processor, the interface module configured to process all communications with the conditional access module and to externally manifest a single virtual processor to the receiver;*
>
> *wherein the interface module receives messages from the receiver, interprets the received messages, and generates first processor messages for the first processor and second processor messages for the second processor, the first processor messages and the second processor messages defining a functional allocation between the first processor and the second processor and wherein the received messages include encrypted data and the functional allocation is time varied according to the encrypted data.*

The Office Action does not indicate where the "interface module" of claim 1 is found in the Schier reference. Presumably, since it refers to this section of the Schier reference:



central processing unit **20**. Engine **30** may comprise a single processing unit or, alternatively, may comprise multiple processing units which are able to perform encryption or decryption using the same or different algorithms simultaneously. The use of such parallel processing capability can greatly enhance the processing throughput of the overall system. Finally, the device **14** includes a timer **32** which may be used in an embodiment of the present invention that is operable to use different encryption techniques in real time communications. This embodiment of the present invention will be described more completely with reference to FIGS. **5** through **7** herein.

the Office Action argues that the interface module is the CPU shown in FIG. 2:

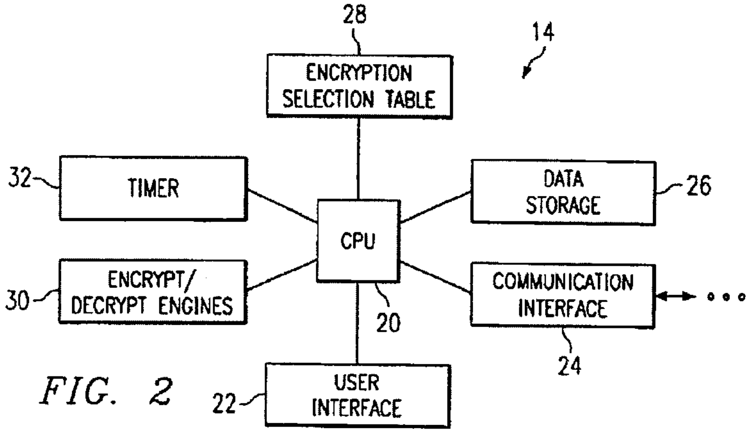
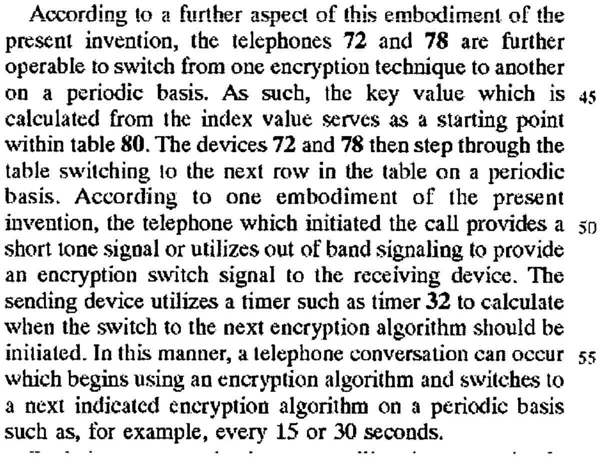


FIG. 2

Claim 1 recites that the interface module (which the Office Action analogizes to the CPU 20) *receives messages from the receiver, interprets the received messages, and generates first processor messages for the first processor and second processor messages for the second processor, the first processor messages and the second* *processor messages defining a functional allocation between the first processor and the second processor and wherein the received messages include encrypted data and the functional allocation is time varied according to the encrypted data.*

According to the Office Action, the features *"wherein the first processor messages and the second processor messages define a functional allocation between the first processor and the second processor, and wherein the functional allocation is time-varying"* is disclosed in the following passage:



> According to a further aspect of this embodiment of the present invention, the telephones **72** and **78** are further operable to switch from one encryption technique to another on a periodic basis. As such, the key value which is calculated from the index value serves as a starting point within table **80**. The devices **72** and **78** then step through the table switching to the next row in the table on a periodic basis. According to one embodiment of the present invention, the telephone which initiated the call provides a short tone signal or utilizes out of band signaling to provide an encryption switch signal to the receiving device. The sending device utilizes a timer such as timer **32** to calculate when the switch to the next encryption algorithm should be initiated. In this manner, a telephone conversation can occur which begins using an encryption algorithm and switches to a next indicated encryption algorithm on a periodic basis such as, for example, every 15 or 30 seconds.

The foregoing discloses an embodiment wherein a call-initiating telephone transmits an out of band encryption switch signal to a call-receiving telephone to indicate when the call-receiving telephone should switch to a different decryption algorithm.

Schier does not disclose a system in which the messages sent to the different encryption engines defines a functional allocation that varies with time. At best, Schier describes a system in which there is an arguable functional allocation (one engine implements one decryption algorithm, the other engine implements another), and one in which messages are routed from one algorithm to another as a function of time, but this is not the same as a *time-varying functional allocation.* In other words, there is an arguable functional allocation and time varying routing of messages, but the functional allocation itself does not change over time.

The Office Action acknowledges that Schier does not teach the functional allocation is time varied according to the encrypted data, but argues that since Wasilewski teaches decryption of control words, one of ordinary skill in the art would have been motivated to modify Schier to perform this function. The Applicant respectfully disagrees.

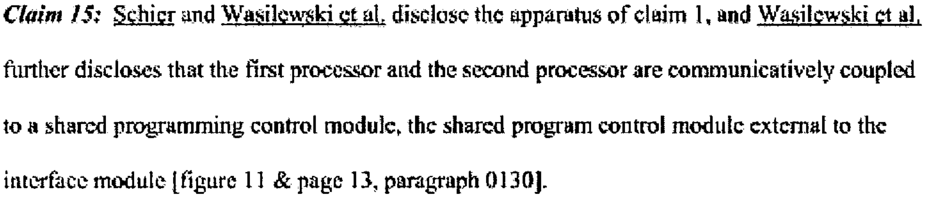
There is no motivation to modify Schier as suggested. Schier teaches using an independent out of band signal to initiate the change from one algorithm to another. All the signal does is initiate the change from one algorithm to another … the algorithm that it is changed to is determined by the table 80, which is secure. There appears to be nothing gained (except further complexity) by the suggested modification. Robustness is not increased, as it would create another possible instrument of failure, nor would it increase the security of the control words.

Claims 19 and 25 are patentable for the same reasons as claim 1, as described above.

With Respect to Claim 15: Claim 15 recites:

> *The apparatus of claim 1, wherein the first processor and the second processor are communicatively coupled to a shared programming control module, the shared program control module external to the interface module.*

According to the Office Action:



> ***Claim 15:*** Schier and Wasilewski et al. disclose the apparatus of claim 1, and Wasilewski et al. further discloses that the first processor and the second processor are communicatively coupled to a shared programming control module, the shared program control module external to the interface module [figure 11 & page 13, paragraph 0130].

The Office Action refers to FIG. 11 of Wasilewski as well as the following text:

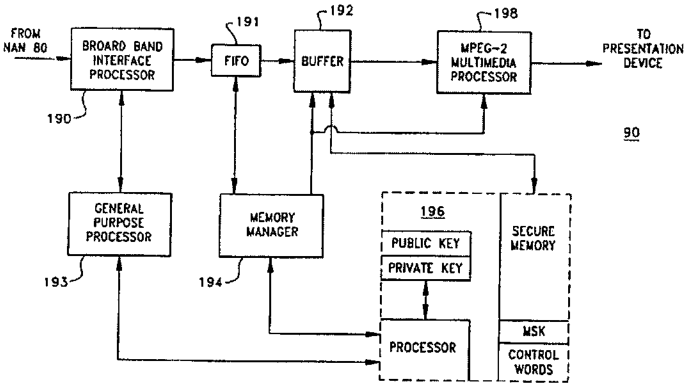
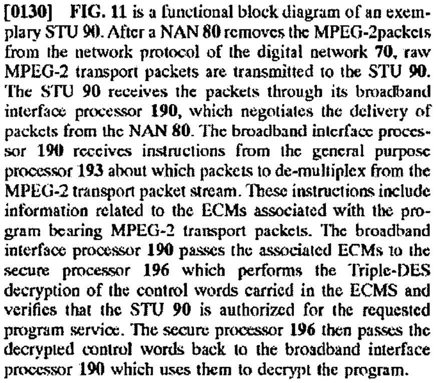


FIG. 11



[0130] **FIG. 11** is a functional block diagram of an exemplary STU **90**. After a NAN **80** removes the MPEG-2packets from the network protocol of the digital network **70**, raw MPEG-2 transport packets are transmitted to the STU **90**. The STU **90** receives the packets through its broadband interface processor **190**, which negotiates the delivery of packets from the NAN **80**. The broadband interface processor **190** receives instructions from the general purpose processor **193** about which packets to de-multiplex from the MPEG-2 transport packet stream. These instructions include information related to the ECMs associated with the program bearing MPEG-2 transport packets. The broadband interface processor **190** passes the associated ECMs to the secure processor **196** which performs the Triple-DES decryption of the control words carried in the ECMS and verifies that the STU **90** is authorized for the requested program service. The secure processor **196** then passes the decrypted control words back to the broadband interface processor **190** which uses them to decrypt the program.

Unfortunately, the Office Action does not indicate which of the claim elements are represented by which of the items shown and described in FIG. 11. The Broadband interface processor negotiates delivery of packets, but does not appear to have anything analogous to the functionality of the claimed interface processor. Nor does FIG. 11 teach or suggest anything analogous to the first and second processors described in claims 1 and 15. Without more, the Applicant cannot agree that Schier and Wasilewski disclose the claimed features, and therefore traverse this rejection.

In paragraph (10), the Office Action rejected claims 3, 17 and 18 under 35 U.S.C. §103(a) as unpatentable over Schier, Wasilewski and Gungle et al., U.S. Patent 5,912,453 (Gungle).

Claims 3, 17, and 18 recite the features of the independent claims they depend upon and are patentable for the same reasons.

In paragraph (12), the Office Action rejected claim 13 under 35 U.S.C. §103(a) as unpatentable over Schier, Wasilewski and Davis, U.S. Patent 6,064,739 (Davis).

Claim 13 recites the features of claim 1, and is patentable for the same reasons

In paragraph (13), the Office Action rejected claim 21 under 35 U.S.C. §103(a) as unpatentable over Schier, Wasilewski and Joly et al., U.S. Patent 7,162,034 (Joly).

Claim 21 recites the features of claim 19 and is patentable for the same reasons.

VI. Dependent Claims

Dependent claims 2-5, 11-18, 21-24, 26 and 27 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicant respectfully requests that these claims be allowed as well.

VII. New Claims

New claims 28-32 are presented for the first time in this Amendment.

Claim 28 recites that the interpreted message includes encrypted data and that the first processor partially decrypts the encrypted data and that the second processor further decrypts the partially decrypted data. Schier discloses the processors being used in parallel or alternatively, not using one processor to partially decrypt the data and the other to further decrypt the partially decrypted data.

Claim 30 recites that the partially decrypted data is provided directly from the first processor to the second processor. Schier teaches away from this embodiment, as all communications are passed through the CPU.

Claim 31 recites that the first processor and second processor perform a decryption operation comprising a set of functions that are allocated to the first microprocessor or the second microprocessor. Claim 31 further recites that multiplication functions are assigned to one processor and addition functions to the other.

None of the cited references disclose these features. For the reasons described above, new claims 28-32 are patentable over the prior art of record, and the Applicant respectfully requests the allowance of these claims as well.

CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

Date: October 10, 2008

By:

Todd N. Snyder, Registration No. 41,320
Attorney for Applicants

The DIRECTV Group, Inc.
CA / LA1 / A109
2230 E. Imperial Highway
El Segundo CA 90245

Telephone No. (310) 964-0560